تكنولوجيا

5 مصطلحات تقنية تتحكم بالخصوصية الرقمية... كيف تحمي نفسك؟

دليل مبسّط لفهم كيف تُجمع بياناتك

المصادقة الثنائية تضيف طبقة حماية إضافية لحساباتك (أرشيفية-رويترز)

واشنطن: «الشرق الأوسط»

نُشر: 09:13-12 يناير 2026 م . 23 رَجب 1447 هـ

حماية المعلومات الشخصية على الإنترنت تبدأ بفهم اللغة الكامنة وراء التطبيقات والأجهزة والحسابات التي تستخدمها. ووفق تقريرٍ نشرته شبكة «فوكس نيوز»، هناك خمسة مصطلحات تقنية أساسية تؤثر مباشرة في الخصوصية الرقمية للفرد، من أذونات التطبيقات (App permissions)، وتتبع الموقع (Location services)، إلى المصادقة الثنائية (Two-factor authentication)، والشبكات الخاصة الافتراضية (VPN)، والإعلانات العابرة للتطبيقات (Cross-app tracking).

يساعد فهم هذه المفاهيم على تقليل تعرّض البيانات للمخاطر والحفاظ على التحكم فيمن يمكنه الاطلاع عليها.

1- أذونات التطبيقات

يطلب كل تطبيق على هاتفك أذونات؛ أيْ موافقات للوصول إلى ميزات مثل الكاميرا أو الميكروفون أو الموقع أو جهات الاتصال أو الصور. بعض هذه الأذونات ضروري لكي يعمل التطبيق، لكن كثيراً من التطبيقات يطلب وصولاً أكبر بكثير مما يحتاج إليه فعلياً.

وبمجرد منح هذه الأذونات، يمكن للتطبيقات جمع البيانات في الخلفية، أحياناً حتى عندما لا تكون تستخدمها بشكل نشط. ومع مرور الوقت، قد يؤدي ذلك إلى تعريض معلومات شخصية حساسة للانكشاف بهدوء ودون أن تشعر.

إن مراجعة أذونات التطبيقات بانتظام وتقييدها من إعدادات هاتفك من أسهل وأكثر الطرق فاعلية لتحسين خصوصيتك. وانتبه، بشكل خاص، للتطبيقات التي لديها حق الوصول إلى موقعك أو الميكروفون أو مكتبة الصور.

2- خدمات تتبع الموقع

تستخدم خدمات تحديد الموقع نظام GPS وشبكات الواي فاي والبلوتوث وأبراج الاتصالات، لتحديد مكانك. ورغم أن ذلك مفيد لتطبيقات الخرائط والطقس، فإن كثيراً من التطبيقات تطلب الوصول الدائم إلى موقعك دون حاجة حقيقية. تقليل صلاحيات الوصول إلى الموقع يحدّ من التتبع ويساعد على حماية خصوصيتك وروتينك اليومي.

3- المصادقة الثنائية

تضيف المصادقة الثنائية طبقة حماية إضافية لحساباتك، إذ تتطلب شيئاً تعرفه (كلمة المرور) وشيئاً تملكه، مثل رمز مؤقت يُرسل إلى هاتفك أو يجري توليده عبر تطبيق مخصص.

حتى لو تمكّن المخترقون من سرقة كلمة مرورك عبر اختراق بيانات أو رسالة تصيّد احتيالي، فإن المصادقة الثنائية يمكن أن تمنعهم من الدخول إلى حساباتك. لهذا السبب، يوصي خبراء الأمن السيبراني بشدة بتفعيلها على حسابات البريد الإلكتروني، والخدمات المصرفية، والتخزين السحابي، ووسائل التواصل الاجتماعي.

قد يستغرق تسجيل الدخول بضع ثوانٍ إضافية، لكن المصادقة الثنائية قادرة على منع سرقة الهوية والوصول غير المصرَّح به، ما يجعلها واحدة من أقوى أدوات الحماية المتاحة اليوم. كلمات المرور القوية والمصادقة الثنائية يعملان بأفضل شكلٍ معاً. إذا كان تذكّر كلمات مرور معقّدة أو إدارة الرموز المؤقتة أمراً مرهقاً، فيمكن لمدير كلمات مرور آمن أن ينشئ كلمات مرور قوية ويخزنها ويملأها تلقائياً بشكل آمن.

4- الشبكة الخاصة الافتراضية

تنشئ الشبكة الخاصة الافتراضية نفقاً آمناً ومشفّراً بين جهازك والإنترنت، ما يخفي عنوان الـIP الخاص بك ويحمي نشاطك على الشبكة من المتطفلين.

تكون الـ«VPN» مهمة، بشكل خاص، عند استخدام شبكات الواي فاي العامة في المطارات أو الفنادق أو المقاهي، حيث يمكن لمُجرمي الإنترنت اعتراض البيانات غير المحمية. كما تساعد أيضاً على الحد من التتبع من قِبل المُعلنين ومُزودي خدمة الإنترنت.

صحيح أن الـ«VPN» لا يجعلك مجهول الهوية تماماً على الإنترنت، لكنه يضيف طبقة قيّمة من الخصوصية والأمان، خاصة عند التصفح أو التسوق أو الدخول إلى حسابات حساسة.

5- التتبع عبر التطبيقات

يتيح التتبع عبر التطبيقات للمعلنين ووسطاء البيانات ربط نشاطك عبر عدة تطبيقات ومواقع. وتُستخدم هذه البيانات لبناء ملفات شخصية مفصلة عنك بناءً على ما تفعله، وتشتريه، وتشاهده.

على أجهزة «أيفون» يخضع هذا النوع من التتبع لنظام شفافية تتبع التطبيقات من «آبل». أما على أجهزة «أندرويد»، فيعتمد على معرّفات الإعلانات وإعدادات تخصيص الإعلانات.

إيقاف هذه الخيارات يحدّ قدرة الشركات على ربط سلوكك عبر التطبيقات المختلفة. ستظل ترى إعلانات، لكنها لن تكون مبنية على نشاطك الشخصي وتفاصيل استخدامك.

مواضيع الإنترنت